APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,955	10/14/2005	Fredrik Lindholm	P18053-US1	2497

27045   7590   05/26/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER
NGUYEN, TRONG H

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
05/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

Office Action Summary	Application No.	Applicant(s)
	10/552,955	LINDHOLM ET AL.
	Examiner	Art Unit
	TRONG NGUYEN	2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2010*.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,13-32 and 34-45* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-11,13-29, 31-32 and 34-45* is/are rejected.

7)☒ Claim(s) *6 and 30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   In view of the Appeal Brief filed on 03/04/2010, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed

by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and

appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth

in 37 CFR 41.20 have been increased since they were previously paid, then appellant

must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by

signing below:

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436

2.   **Claims 1-11, 13-32 and 34-45** are currently pending.

3.   Applicant's arguments, with regards to claims 1-11, 13-32 and 34-45, filed

03/04/2010 have been fully considered but they are not wholly persuasive. While

Applicants argue that their invention does not require a common authentication server

(bottom of page 5 and top of page 7), this feature is not recited in the claims. Specifically, claim 1 recites "a group of at least two units" however a "unit" can be any entity including a common authentication server.

Allowable Subject Matter

4.   **Claims 6 and 30** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims as well as overcoming any objection(s) and/or rejection(s) set forth below.

Claim Objections

5.   **Claim 1, 10, 32, 43 and 45** are objected to because of the following informalities:

"the steps of;" on lines 3 and 9 of claim 1 should be "the steps of:"

"the steps of;" on line 2 of claim 10 should be "the steps of:"

"comprises;" on line 2 of claim 32 should be "comprises:"

"comprising;" on line 1 of claim 43 should be "comprising:"

"comprises;" on line 2 of claim 45 should be "comprises:"

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 10-11, 13, 39 and 42-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 10 recites "the token secret" on last line however it is unclear whether "the token secret" refers to "a token secret" recited on line 10 of claim 1 or "a token secret" recited on line 3 of claim 10. Similar issue also exists in claims 11 and 13.

Claim 39 recites "wherein policies defining critical operations for which authentication is needed" which is unclear. For examining purposes, it will be interpreted similarly to claim 21.

Claims 42-45 recite "the device" on line 1 however it is unclear whether "the device" refers to "first device" or some other device in "a group of at least two devices" in claim 41.

Claim 45 recites "the token secret" on last line however it is unclear whether "the token secret" refers to "a token secret" recited on line 12 of claim 41 or "a token secret" recited on line 3 of claim 45.

Claim Rejections - 35 USC § 101

7.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1 is rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or

materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008);

Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584,588 n.9

(1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S.

780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process

would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory

process, the claim should positively recite the particular machine to which it is tied, for

example by identifying the apparatus that accomplishes the method steps, or positively

recite the subject matter that is being transformed, for example by identifying the

material that is being changed to a different state.

Here, applicants' method steps are not tied to a particular machine and do not

perform a transformation. Thus, the claim is non-statutory.

The mere recitation of the machine in the preamble with an absence of a

machine in the body of the claim fails to make the claim statutory under 35 USC 101.

Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.

Claims 2-11 and 13-24 are rejected under 35 U.S.C. 101 as non-statutory for at

least the reason stated above. Claims 2-11 and 13-24 depend on claim 1; however,

they do not add any feature or subject matter that would solve any of the non-statutory

deficiencies of claim 1.

Claim Rejections - 35 USC § 102

8.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9.   **Claims 1, 10-11, 13, 15-21, 23, 25, 32, 34-41 and 45** are rejected under 35

U.S.C. 102(e) as being anticipated by Jablon US 6,792,533 B2 (hereinafter "Jablon").

        Regarding claim 1, Jablon discloses **a method for password-based**

authentication in a communication system including a group of at least two units

[Fig. 5, col. 18, lines 55-59: authenticating Alice to Bob, where Bob is the host computer

and Alice is the user's computer] **associated with a common password,** [Fig. 5: 501 C

= shared password] **comprising the steps of**;

        assigning individual authentication tokens [col. 19, line 65 - col. 20, line 2:

each of Alice and Bob is assigned a one way hidden password S = H_C (g)] **to the**

respective units in the group based on the password such that each

authentication token is irreversibly determined by the password; [col. 19, line 65 –

col. 20, line 2: the one way hidden password S = H_C (g) is a one way function of the

shared password C]

determining, at a first unit, a check token [Fig. 5, 505: W = proof (K$_1$, K$_2$)] **for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;**

determining, at the first unit, a token secret [Fig. 1 and col. 20, lines 3-5: the shared authenticated key K$_1$ is generated by Alice in the SPEKE exchange using the one way hidden password S which is a one way function of shared password C] **using the authentication token of the first unit and the password**; and,

creating, at the first unit, the check token [Figs. 1 and 5, 505, col. 20, lines 3-20: Alice computes W = proof (K$_1$, K$_2$) where the shared authenticated key K$_1$ is generated in the SPEKE exchange using the one way hidden password S which is a one way function of shared password C] **for the second unit based on the token secret and the password**;

sending the check token to the second unit; [Fig. 5: 509 Alice sending W to Bob] and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit. [Fig. 5, 515-517: after receiving W from Alice 509, Bob verifies that W proves that she knows both K$_1$ and K$_2$

515. If the verification succeeds, Bob has proven that Alice knows C and the protocol

succeeds 517]

Regarding <u>claim 10</u>, Jablon further discloses **the method of claim 1, wherein
the assigning step further comprises the steps of**;

**determining, at an assigning unit in the group, a token secret common for
the group and non-correlated with the password**; [col. 19, lines 48-49: some fixed
value g known to Bob and Alice] and,

**creating, at the assigning unit, the authentication token for another unit in
the group based on the token secret and the password** [col. 19, line 65-67: Alice
computes the one way hidden password $S = H_C (g)$]

Regarding <u>claim 11</u>, Jablon further discloses **the method of claim 10 wherein
the step of determining the token secret involves generating the token secret, as
part of an initial set-up procedure** [col. 19, line 64: at time of password setup]

Regarding <u>claim 13</u>, Jablon further discloses **the method of claim 10, wherein
the creating step involves using a bijective locking function, the input parameters
of which include the token secret and a one-way function of the password** [col. 7,
lines 5-12 and col. 19, line 65-67: Alice computes the one way hidden password $S = H_C$
(g)]

Regarding <u>claim 15</u>, Jablon further discloses **the method of claim 13, wherein the locking function is implemented through password-based secret sharing** [col. 7, lines 5-12 and col. 19, line 65-67: Alice computes the one way hidden password $S = H_C (g)$]

Regarding <u>claim 16</u>, Jablon further discloses **the method of claim 1, wherein implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts** [col. 12, lines 8-17: logging failed attempts, counting the number of failed attempts over the lifetime of the password, disabling the password if a specific limit is exceeded, and temporarily disabling the account during a suspected attack count total failed attempts to detect attacks against anonymous accounts]

Regarding <u>claim 17</u>, Jablon further discloses **the method of claim 1, further comprising the step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value** [col. 12, lines 8-17: logging failed attempts, counting the number of failed attempts over the lifetime of the password, disabling the password if a specific limit is exceeded, and temporarily disabling the account during a suspected attack count total failed attempts to detect attacks against anonymous accounts]

Regarding **claim 18,** Jablon further discloses **the method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating the result of the comparing step** [Fig. 5, Abort 516 or OK 517]

Regarding **claim 19**, Jablon further discloses **the method of claim 1, further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other** [col. 22, lines 37-40, col. 23, lines 19 and 23: Bob is verified and Alice is verified]

Regarding **claim 20**, Jablon further discloses **the method of claim 19, further comprising the steps of:**

generating a respective random value at the first and second unit; [col. 23, lines 8 and 10: Bob generates a random integer R_B, Alice generates random integer R_A]

determining temporary test secrets at the first and second unit based on the random values; [col. 23, lines 8 and 12: Bob generates $Q_B = h\ (S)^{(2\ R_B)}$ mod p and Alice generates $Q_A = h\ (S)^{(2\ R_A)}$ mod p] and,

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes [col. 23, lines 8 and 13: Bob sends Q_B to Alice and Alice sends Q_A to Bob]

Regarding **claim 21**, Jablon further discloses **the method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units** [col. 24, lines 1-14: Since passwords are ubiquitous, this invention has broad applications. It is useful for enhanced security in situations where passwords or PINs are traditionally used, such as remote personal-computer banking, authenticating access for portable telephones, and in general, remote secure financial and other transactions. It is also suitable for general computer network login procedures, where the security of the underlying network may not be entirely trusted]

Regarding **claim 23**, Jablon further discloses **the method of claim 1, wherein the group of units constitutes a Personal Area Network (PAN)** [Fig. 1 or 5]

Regarding **claim 25**, this claim contains limitations that are substantially similar to those recited in claim 1 above and accordingly is rejected for similar reasons.

Regarding **claim 32**, this claim contains limitations that are substantially similar to those recited in claim 10 above and accordingly is rejected for similar reasons.

Regarding **claim 34**, this claim contains limitations that are substantially similar to those recited in claim 13 above and accordingly is rejected for similar reasons.

Regarding <u>claim 35</u>, this claim contains limitations that are substantially similar to those recited in claim 16 above and accordingly is rejected for similar reasons.

Regarding <u>claim 36</u>, this claim contains limitations that are substantially similar to those recited in claim 17 above and accordingly is rejected for similar reasons.

Regarding <u>claim 37</u>, this claim contains limitations that are substantially similar to those recited in claim 18 above and accordingly is rejected for similar reasons.

Regarding <u>claim 38</u>, this claim contains limitations that are substantially similar to those recited in claim 19 above and accordingly is rejected for similar reasons.

Regarding <u>claim 39</u>, this claim contains limitations that are substantially similar to those recited in claim 21 above and accordingly is rejected for similar reasons.

Regarding <u>claim 40</u>, this claim contains limitations that are substantially similar to those recited in claim 23 above and accordingly is rejected for similar reasons.

Regarding <u>claim 41</u>, this claim contains limitations that are substantially similar to those recited in claim 1 above and accordingly is rejected for similar reasons.

Regarding **claim 45**, this claim contains limitations that are substantially similar to those recited in claim 10 above and accordingly is rejected for similar reasons.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11.   **Claims 2, 26 and 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Uskela US 6,721,886 (hereinafter "Uskela").

Regarding **claim 2**, Jablon discloses **the method of claim 1** but does not specifically disclose **further comprising the step of: deleting the password and all significant parameters generated except the authentication tokens after usage thereof**.

However, Uskela discloses a method for preventing unauthorized use of services wherein authentication, verification, and user data generated during authentication are deleted from memory after authentication (Col. 5, lines 40-43).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the time of the invention to modify the invention of Jablon by deleting sensitive data such as user data (password), authentication and verification data (intermediate

parameters) generated during authentication after usage except provided

authentication tokens as described by Uskela since it would provide a safety measure

against the security risk (Uskela, Col. 5, lines 39-40).

Regarding claim 26, this claim contains limitations that are substantially similar

to those recited in claim 2 above and accordingly is rejected for similar reasons.

Regarding claim 42, this claim contains limitations that are substantially similar

to those recited in claim 2 above and accordingly is rejected for similar reasons.

12.   **Claims 3, 5, 27, 29 and 43** are rejected under 35 U.S.C. 103(a) as being

unpatentable over Jablon in view of Hauser et al. US 5,778,065 (hereinafter "Hauser").

Regarding claim 3, Jablon discloses **the method of claim 1** but does not

specifically disclose **further comprising the step of: accepting, at the second unit**

in response to a successful authentication, update information securely

transferred from the first unit, at least a portion of the update information being

created at the first unit.

However, Hauser discloses an authentication server in response to a successful

authentication, accepting update information (new key or password) securely

transferred (encrypted under present key) from a user and the update information is

created by the user (Col. 2, lines 31-32, 34-36, and 44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by having the second unit accepting update information securely transferred from the first unit in response to a successful authentication as described by Hauser for security reasons since passwords or keys are necessary to communicate safely between users or between users and servers (Hauser, Col.1, lines 13 and 22-24).

Regarding <u>claim 5</u>, Jablon-Hauser combination further discloses **the method of claim 3**, **wherein the update information relates to a password change** [Hauser, Col. 7, lines 10-11: discloses a user requesting a password change or update with an authentication server].

Regarding <u>claim 27</u>, this claim contains limitations that are substantially similar to those recited in claim 3 above and accordingly is rejected for similar reasons.

Regarding <u>claim 29</u>, this claim contains limitations that are substantially similar to those recited in claim 5 above and accordingly is rejected for similar reasons.

Regarding <u>claim 43</u>, this claim contains limitations that are substantially similar to those recited in claim 3 above and accordingly is rejected for similar reasons.

13.   **Claims 4 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of Aiello et al. US 6,397,329 (hereinafter "Aiello").

     Regarding <u>claim 4</u>, Jablon-Hauser combination discloses **the method of claim 3** but does not specifically disclose **wherein the update information is associated with revocation of a non-trusted group member**.

     However, Aiello disclose a certificate authority (CA) periodically generates and signs a complete certificate revocation list (CRL) or a modification of a previous list or revoked certificates (Col. 4, lines 13-16).

     Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser by having the update information associating with revocation of a non-trusted group members as described by Aiello since it would provide for the purpose of verifying the authenticity of a presented identity (Aiello, Col. 6, lines 23-24).

     Regarding <u>claim 28</u>, this claim contains limitations that are substantially similar to those recited in claim 4 above and accordingly is rejected for similar reasons.

14.   **Claims 7-8, 31 and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of Matsumoto US 6,215,877 (hereinafter "Matsumoto").

Regarding <u>claim 7</u>, Jablon-Hauser combination discloses **the method of claim
3** but does not specifically disclose **further comprising the step of delegating
update rights to a third intermediate unit, and sending at least a portion of the
update information for the second unit to the intermediate unit**.

However, Matsumoto disclose a key management server generates a new
channel secret key for a chat client, delegates update rights (right to transmit the new
key to the chat client) to a chat server and transmits this newly generated channel
secret key to the chat server to be sent to a chat client (Fig. 6, Col. 1, lines 61-64 and
Col. 10, lines 45-49).

Therefore, it would have been obvious to a person of ordinary skill in the art at
the time of the invention to modify the invention of Jablon-Hauser by delegating update
rights to a third intermediate unit as described by Matsumoto since it would provide for
the purpose of preventing eavesdropping (Matsumoto, Col. 1, lines 42-44).

Regarding <u>claim 8</u>, Jablon-Hauser-Matsumoto combination further discloses **the
method of claim 7, wherein the update information is accompanied by a time
stamp for determining whether the update information is still valid when the
intermediate unit encounters the second unit** as [Matsumoto, Col. 10, lines 45-49:
discloses the deadline of the key is written in the channel secret key for determining
the validity of the channel secret key. In addition, Hauser, Col. 2, lines 33 and 43-44:

also discloses including freshness information in update information to determine its validity].

Regarding <u>claim 31</u>, this claim contains limitations that are substantially similar to those recited in claim 7 above and accordingly is rejected for similar reasons.

Regarding <u>claim 44</u>, this claim contains limitations that are substantially similar to those recited in claim 7 above and accordingly is rejected for similar reasons.

15.   **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser, further in view of Matsumoto, and further in view of Gunter et al. US 6,885,388 (hereinafter "Gunter").

Regarding <u>claim 9</u>, Jablon-Hauser-Matsumoto combination discloses **the method of claim 7** but does not specifically disclose **wherein the delegation of update rights comprises delegation of rights to further delegate update rights**.

However, Gunter discloses delegation of permission comprises the authority to delegate one or more further permissions to subsequent delegates (Col. 2, lines 40-41).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser-Matsumoto by having delegation of update rights comprises delegation of rights to further delegate as

described by Gunter since it would provide for the purpose of secure and convenient distribution of sensitive content and services (Gunter, Col. 2, lines 23-24).

16.   **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Brainard et al. US 7,363,494 (hereinafter "Brainard").

Regarding claim 14, Jablon discloses **the method of claim 13** but does not specifically disclose **wherein the locking function is a symmetric encryption function**.

However, Brainard discloses that an authentication code may be generated by a block cipher which encrypts a hash value of a shared password and/or other additional values using a stored secret (K) (Brainard, Col. 10, lines 58-61, Col. 14, lines 65-67, and Col. 15, lines 1-2)].

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by having the locking function being a symmetric encryption function as described by Brainard since it is well known in the art.

17.   **Claim 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of Hauser and further in view of McDowell et al. US 6,668,167 (hereinafter "McDowell").

Regarding claim 22, Jablon-Hauser combination discloses **the method of claim 3** but does not specifically disclose **wherein a unit that is switched-on after**

being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

However, McDowell discloses a MS that is turned on after being inactive for a predetermined period of time automatically requests update information (new TMSI) from the MSC and VLR (Fig. 14, Col. 10, lines 54-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon-Hauser by having a unit after switched-on automatically requests update information as described by McDowell since it would provide for the purpose of receiving important update information (McDowell, Col. 10, lines 54-55).

18.   **Claim 24** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon in view of MacKenzie US 7,076,656 (hereinafter "MacKenzie").

Regarding <u>claim 24</u>, Jablon discloses **the method of claim 1** but does not specifically disclose **wherein the authentication tokens are tamper-resistantly stored in the respective units**.

However, MacKenzie discloses persistent stored data being tamper-proof (Col. 2, lines 22-26).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Jablon by tamper-proofing stored authentication codes (persistent stored data) in respective units as described by

MacKenzie since it would provide extra security against attack by adversaries (MacKenzie, Col. 2, lines 27-29).

Conclusion

19.   Examiner cites particular pages or columns or paragraphs and/or line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, applicant fully considers the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

20.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/   /T N/
Supervisory Patent Examiner, Art Unit 2436   Examiner, Art Unit 2436